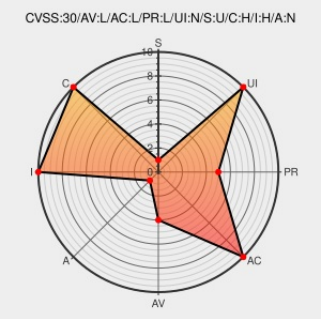
CVE-2016-10330

Published on: 05/12/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:01 PM UTC

CVE-2016-10330

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Photo Station from Synology contain the following vulnerability:

Directory traversal vulnerability in synophoto_dsm_user, a SUID program, as used in Synology Photo Station before 6.5.3-3226 allows local users to write to arbitrary files via unspecified vectors.

CVE-2016-10330 has been assigned by security@synology.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Synology** - **Synology Photo Station** version **All versions prior to version 6.5.3-3226**

CVSS3 Score: 7.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
bamboofox official blog	Exploit Third Party Advisory bamboofox.github.io	MISC bamboofox.github.io/2017/03/20/Synology-Bug-Bounty-2016/#Vul-04-Privilege-Escalation

	text/html Inactive Link Not Archived	
bamboofox official blog	Exploit Third Party Advisory bamboofox.github.io text/html Inactive Link Not Archived	MISC bamboofox.github.io/2017/03/20/Synology-Bug-Bounty-2016/#Vul-03-Read-Write-Arbitrary-Files
oss-sec: CVE request: Synology Photo Station command injection and privilege escalation	Exploit Third Party Advisory VDB Entry seclists.org text/html	MLIST [oss-security] 20160128 CVE request: Synology Photo Station command injection and privilege escalation
Photo Station 6.5.3-3226 | Synology Inc.	Release Notes www.synology.com text/html	Syno CONFIRM www.synology.com/en-global/support/security/Photo_Station_6_5_3_3226

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Synology	Photo Station	All	All	All	All

cpe:2.3:a:synology:photo_station:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→